1. A method for encrypting data, the method comprising:

providing a data source, configured to receive initialization parameters and an offset and to output data corresponding to the initialization parameters, the number of times data is output by the random number source, and the offset;

inputting initialization parameters to the random data source;

providing an input store comprising memory storing input data ;

providing an output store comprising memory for storing output data; and

executing a substitution process, the substitution process, comprising

outputting a byte length from the random data source,

reading an input string having an input string length from the input store having a length corresponding to the bit length,

inputting the input string as the offset to the data source,

outputting a cipher string from the data source having a length equal to the input string length, and

writing the cipher string to the output store.

2. The method of claim 1, further comprising:

providing an in-process buffer;

writing the cipher string to the in-process buffer; and

performing an obfuscation operation on the cipher string if a first test condition exists.

3. The method of claim 2, further comprising

providing a test pattern;

providing a determination pattern;

and wherein the first test condition is the equality of the test pattern and a portion of the determination pattern.

4. The method of claim 3, further comprising:

outputting an obfuscation code from the data source; and

wherein performing the obfuscation operation comprises performing a manipulation corresponding to the obfuscation code;

5. The method of claim 4, further comprising:

outputting an obfuscation length from the data source; and

wherein performing the obfuscation operation further comprises, performing the manipulation on a portion of the cipher text having a length corresponding to the obfuscation length.

6. The method of claim 5, wherein the manipulation is at least one of an exclusive or, a shift, and a substitution.

7. The method of claim 6, further comprising:

repeatedly resetting the test pattern and the determination pattern; and repeatedly performing the obfuscation operation if the first test condition continues to exist.

8. The method of claim 7, further comprising:

inserting an insertion pattern if a second test condition exists.

9. The method of claim 8, wherein inserting an insertion pattern further comprises:

resetting the test pattern and the determination pattern; and

wherein the second test condition is the equality of the test pattern and a portion of the determination pattern.

10. The method of claim 9, wherein the data source is a random pattern generation machine.

11. The method of claim 9, wherein the data source comprises a plurality of random pattern generation machines and an aggregate heterogeneous bit pattern.

12. The method of claim 9, wherein the random pattern generation machine comprises a pattern table and a logical base and wherin outputting a pattern from the data source comprises, outputting a pattern from the pattern table corresponding to the logical base and advancing the logical base.

13. The method of claim 12, wherein advancing the logical base comprises modifying the current value according to a rule to obtain a result and storing the result as the logical base.

14. The method of claim 13, wherein the plurality of RPGMs comprises a selection RPGM and a plurality of cipher RPGMs, and wherein

outputting a bit length further comprises outputting a selection pattern from the selection RPGM, the selection pattern corresponding to one of the plurality of cipher RPGMs; and

outputting a cipher string from the data source further comprises outputting a pattern from the cipher RPGM corresponding to the selection pattern output from the selection RPGM

15. The method of claim 14, wherein the selection RPGM is also a cipher RPGM.

16. A method for encrypting and decrypting data, the method comprising:

providing a first computer;

storing on the first computer a first data source having a logical base and an offset, the data source configured to output a cipher pattern corresponding to the logical base and the offset and configured to advance the logical base;

setting the logical base equal to an initial value;

providing a plurality of clear text segments;

encrypting each clear text segment, encrypting comprising

substituting for subsegments of the clear text segment, substituting for subsegments comprising,

selecting a subsegment length,

reading a subsegment from the clear text segment having a length equal to the bit length,

setting the offset equal to a value corresponding to the subsegment,

outputting a cipher pattern from the first data source,

writing the cipher pattern to an output buffer, and

advancing the logical base;

repeatedly, substituting segments for the entire message segment;

providing a second computer;

storing on the second computer a second data source substantially identical to the first data source and further configured to output the offset corresponding to the logical base thereof and a cipher pattern;

transmitting the initial value of the logical base to a second computer;

transmitting the cipher patterns to the second computer;

decrypting each cipher pattern, decrypting comprising,

for each cipher pattern, creating a substitution record corresponding to the cipher pattern,

storing the value of the logical base in a substitution record, and

advancing the logical base, and

for each substitution record, outputting the value of the offset from the data source corresponding to the value of the logical base and cipher pattern of the substitution record; and

writing the clear text patterns to an output buffer.

17. A method for encrypting and decrypting data, the method comprising:

providing a first computer storing a first data source configured to output patterns corresponding to at least one of an offset and a logical base, the first data source further configured to advance the logical base upon outputting a pattern;

providing a clear text store storing clear text;

providing a cipher text store for storing cipher text

setting the logical base equal to an initial value;

encrypting the clear text, encrypting comprising, for substantially all the clear text,

selecting a clear text segment from the clear text,

substituting a cipher text segment for clear text segment according to substitution parameters output from the first data source having the offset thereof set equal to the clear text segment,

storing the cipher text segment in an output buffer,

obfuscating the cipher text segment according to obfuscation parameters output from the first data source, and

writing the cipher text segment to the cipher text store;

providing a second computer storing a clear text store and a second data source configured to output patterns corresponding to at least one of an offset and a logical base, the second data source further configured to advance the logical base upon outputting a pattern;

transmitting the initial value to the second computer;

setting the logical base of the second data source equal to the initial value;

transmitting the contents of the cipher text store to the second computer; and

decrypting the contents of the cipher text store, decrypting comprising, for each cipher text segment:

selecting a cipher text segment from the cipher text store,

outputting substitution parameters from the data source,

creating a substitution record storing the substitution parameters,

outputting obfuscation parameters from the data source,

creating an obfuscation record storing obfuscation parameters,

processing the obfuscation record to undo the obfuscation,

processing the substitution record to obtain clear text,

writing the clear text to the clear text store.

18. A method for outputting a random number, the method comprising:

providing a computer comprising a memory for storing executable and operational data structures and a processor operably connected to the memory;

providing a plurality of distribution RPGMs each having an RPGM identifier, a pattern table, and a logical base, the pattern table of each RPGM containing patterns having a distribution corresponding to a portion of a distribution;

providing a selection RPGM having a pattern table and a logical base stored in the memory, the pattern table of the selection RPGM storing a plurality of values, each value being equal to one of the RPGM identifiers, with the number of values equal to any one of the RPGM identifiers equal to the number of patterns within the pattern table of the distribution RPGM corresponding to that RPGM identifier;

outputting a selection pattern from the pattern table of the selection RPGM;

outputting an output pattern from a selected RPGM, the selected RPGM being the distribution RPGM corresponding to the selection pattern;

advancing the logical bases of the selection RPGM and the selected RPGM.